REMARKS

Claims 25 to 60 are in the application of which claims 25, 36, 37 and 60 are independent claims. In our response to the action, we will focus on these independent claims.

We believe that it will be helpful, first, to review the disclosure of Rosen (US 5,557,518) before going on to consider the distinctions between the claimed invention and the technique described in that patent.

The basic concept of Rosen is shown in patent Figure 1. A customer and a merchant each have a trusted agent and a money module.

A trusted agent is a tamperproof combination of hardware and software (column 4, lines 9-11). The money module includes a money holder (column 22, lines 25-27) which contains electronic representations of money.

The customer's money module sends electronic money to the merchant's money module in return for electronic merchandise (column 4, lines 34-38). The electronic merchandise (not the money) consists of a ticket, optionally associated with an encrypted electronic object (column 4, lines 41-44). The features of a ticket (that is electronic merchandise) are described with reference to Figure 2 at column 5, line 38 to column 7, line 61. It is noted that although several different embodiments of tickets are described, none of the tickets represents money. The closest Rosen approaches money is a purchase order or invoice for specific items (column 6, lines 44-50).

It is further noted that a ticket does not include within itself an identifier for the ticket. Identifier Section 10 holds information that identifies the merchant or authority creating the ticket (column 5, lines 44-46). A decryption ticket includes an object identifier field 36, which uniquely identifies a particular electronic object (column 5, lines 59-61), but the Examiner will recognize that identifying the object to be decrypted, for example a moving, is not the same as identifying the ticket itself. Furthermore it can be seen by inspection of Figure 2 that none of the fields within a ticket includes a ticket identifier. Ticket transfer between trusted agents is described at column 25, line 64 to column 6, line 39, with reference to Figure 25. Step 856 of Figure 24A shows that ticket holder A, which here is transferring a ticket to B, must request ticket IDs from a host. It can therefore be seen that the tickets described in Rosen do not include a ticket identifier.

Rosen does not explicitly disclose a document carrier either. The closest approximation to a document carrier appears to be a trusted agent which, as has previously been noted, comprises a combination of hardware and software and which is tamper proof. Thus, the Examiner may consider that the closest approximation to the document carrier identifier is a trusted agent identifier. A trusted agent identifier (TA) ID is described in Rosen at column 11, lines 14-16 and forms part of a trusted agent certificate (column 11, lines 20-21; column 11, line 50). But it can be seen from inspection of Figure 2 and from the description at column 5, line 38 to column 7, line 61

that a trusted agent identifier does not form part of any of the tickets disclosed in Rosen.

Before going on to highlight some of the patentable distinctions the presently claimed invention provides over Rosen, it is useful to review the operation of the Rosen procedure. Rosen describes the procedure using flow charts which define a number of routines and sub routines. An important sub routine is the Establish Session sub routine (column 13, lines 30-34) which is used a number of times to create secure encryption channels between trusted agents and other trusted agents, trusted agents and trusted servers, a trusted agent and its associated money module, and between money modules (column 15, lines 21-23; column 16, lines 9-13; column 16, lines 49-51; column 17, lines 61-63; column 19, lines 62-65; column 20, lines 31-36). The basic Establish Session procedure is described with reference to Figure 9 in the context of setting up a secure channel between a trusted agent and a trusted server, at column 15, line 21 up to column 16, line 51. This procedure is reviewed further below. The basic concept behind Rosen is that of an abort and commit procedure in which electronic notes are provisionally passed from a customer to a merchant in payment for an electronic ticket which is provisionally passed from the merchant to the customer, both sides then committing to (or aborting) the transaction (column 13, line 38 to column 15, line 11, in particular column 14, line 24 to line 47).

The outline procedure is as follows:

A trusted agent is initialized by having a unique identification assigned to it (column 11, lines 15-17) and the agent then generates a key pair, passes the public key to a trusted server which incorporates this into a certificate for the trusted agent and passes this back (column 11, lines 18-23, and line 50). The certificate includes a signature of the trusted server issuing the certificate (column 11, line 50) and this signature comprises an encryption operation on a hash function (column 12, line 12) in combination with column 12, lines 8-9 and column 11, line 58). The data that is signed (by hashing then encrypting) is data "Y" as identified in column 11, line 51, comprising TA (id) || TA (PK) || expire data.

The purchase of electronic merchandise is described in column 7, line 43 to column 23, line 51. In outline, this involves setting up four secure, encrypted channels, as shown in Figure 13, one 436 between a pair of trusted agents, two more 438, 440 between each trusted agent and its money module, and a further tunneled encryption session 442 between a pair of money modules (column 17, line 64 to column 18, line 4). Thus communication between money modules is double encrypted (column 21, lines 47-54; column 20, lines 26-30).

The way in which a session is established between trusted agents is substantially the same as the way in which a session is established between money modules (column 20, lines 31-33). The basic Establish Session sub routine is described at column 15, line 21 to column 16, line 51 in the context of the secure communication of a message between a trusted server and a trusted agent using a session key (TA/TA) and this de-

scription is then referred to later, for example at column 17, lines 61-63 (trusted agents are periodically re-certified - column 12, lines 22-24).

Referring now to the established session sub routine, it will be seen from the review below that this establishes a symmetric cryptographic session where both parties share the same session key. This is also clearly implicit in the references to a single session key for each communication channel shown in Figure 13, and is the reason for both public key and symmetric key cryptographic functions 151 of the trusted agent of Figure 4A (column 9, lines 56-58).

The mechanism for establishing a shared (symmetric) session key between A and B is described at column 15, line 45 to column 16, line 32. B sends A a random number, encrypted with A's public key; A then generates a second random number and sends this to B encrypted with B's public key. At this point, A and B both know both random numbers and these are exor'd together to create a session key. In fact, B's message to A includes B's certificate and vice-versa.

Once the various secure links shown in Figure 13 have been established (column 21, lines 5-6) goods (a ticket) are provided to the customer (A) and the customer's money module then transfers electronic notes in the amount specified to the merchant's (B) money module for payment (column 22, lines 37-39).

It is important to note that the possibility of duplication for loss is minimized by the order and timing of A's and B's committing to a given transaction, as previously outlined (column 14, lines 7-11). The precise procedure for transferring a ticket is de-

scribed at column 25, line 64, to column 26, line 39 with reference to Figure 25). In outline, the trusted agents establish a secure session (column 26, line 14), a selected ticket is then signed over from A to B by adding appropriate transfer information to the Transfer History section and appending the digital signature to the Sender Signatures section (column 26, lines 26-28) and the ticket is then sent to B for validation.

Having reviewed the operation of the closest prior art procedure, significant distinctions of the claimed invention from this procedure will now be explained.

Independent Claim 25

The Examiner's rejection of the patentability of this claim in view of Rosen is respectfully contested.

This claim recites a method of issuing an electronic negotiable document (END). It can be seen from the description in the present application, for example the paragraph spanning pages 11 and 12, that an END includes electronic cash and, broadly speaking, represents money; other examples given include bank checks, bills of lading, and bills of exchange. The Examiner, in paragraph 3 of the Official Action, appears to agree, referring to an electronic negotiable document... i.e. "*electronic money*" (paragraph 3, line 5). However, the Examiner goes on to refer to features of tickets, that is electronic merchandise, in contesting the patentability of Claim 25 (see for example paragraph 3, line 8). From the foregoing discussion it will be appreciated, however, that in Rosen a ticket, that is electronic merchandise, is not the same as electronic money. Nonetheless it will be explained below that whether an END is considered to

be electronic money or a ticket, Claim 25 recites novel and non-obvious features neither taught nor suggested by the prior art.

To avoid undue prolixity the applicant will focus upon the main features of distinction over the prior art:

Claim 25 recites a method of issuing an electronic negotiable document. Rosen does not teach or suggest any methods of issuing such a document – instead Rosen assumes that a ticket or electronic money has already been issued and concerns itself with the transfer of tickets and money between trusted agents and money modules. Rosen describes the Issuer Signature section of a ticket (column 7, lines 29-41) but assumes a ticket has been issued (column 7, line 44) and nowhere describes the issuing procedure. Rosen merely describes how an already issued ticket is transferred from one trusted agent to another (column 7, lines 56-59; column 25, line 64 to column 26, line 39). Likewise, Rosen in completely silent on how electronic money is issued, instead describing protocols for managing the transfer of electronic representations of money (see, for example, column 38, line 24 to column 39, line 3) which describes the transfer of notes but is entirely silent on how these notes are issued initially. Rosen describes in detail how a trusted agent is initialized and re-certified (see, for example, column 11, lines 13-30) but neither teaches nor suggests any procedures for issuing an electronic negotiable document.

Even were the transfer of tickets or notes from one trusted agent to another to be considered a form of issue, as will be seen below, a number of significant features of the claimed method of issuing are neither taught nor suggested by Rosen.

Claim 25 also recites an END identifier, which is signed. Rosen entirely lacks such an END identifier, whether an END is considered as a ticket (see above explanation of the lack of a ticket identifier in Rosen) or money.

Moreover, Rosen neither teaches nor suggests a method of issuing an END comprising creating a unique document carrier identifier, still less the signing of this identifier. When a ticket is created, for some types of ticket an Object Identifier field by may be created, but this does not identify the trusted agent which will carry the ticket. Rosen is entirely silent on how electronic money may be issued.

The claimed invention thus recites a method of issuing an electronic negotiable document comprising, *inter alia*, creating the END and a unique document carrier identifier and then signing the unique document-carrier identifier, the END and an END identifier. Such a method of issuing provides a combination of signed features which neither taught nor suggested by Rosen or any of the other prior art documents, either alone or in combination.

Dependent Claims Dependent Upon Claim 25

Claims 26 to 35 and 46 to 51 being dependent upon Claim 25 are allowable for the same reasons.

Further, the Examiner's initial views as to the patentability of the features recited in these dependent claims is respectfully contested.

In particular, dependent Claims 27 and 30 both refer to calculating a hash value of data prior to signing. The Examiner refers to column 12, lines 6-8 in respect of Claim 27, but this refers back to the generation of a certificate for a trusted agent and not to the issuing of an electronic negotiable document. In respect of Claim 30 the Examiner refers to column 11, lines 62-67 and column 12, lines 6-16, for which the same comments apply - this refers to a certificate for a trusted agent not to a method of issuing an END with features as claimed.

Independent Claim 36

The applicant will here focus on two significant, and it is submitted patentable, distinctions of the claimed method of negotiating an END over the disclosures of Rosen considered alone or combination with the secondary references.

Applicant's claimed method of negotiating employs a negotiability status flag indicative of whether the END is currently negotiable from the document carrier on which it is stored; this flag is set at the end of the procedure to "negotiable" and "non-negotiable" for the recipient and provider of the END respectively. It is respectfully submitted that such a feature is neither taught nor suggested in Rosen - instead Rosen uses an abort and commit procedure to achieve similar results - that is to minimize the possibility of duplication (column 14, lines 7-11). Because Rosen uses a different procedure to achieve the desired end, there is no need for a negotiability flag (or a counter

to perform a similar function - see argument re: Claim 37 below). If an END is taken to include a ticket then it might be considered that an In Use field of the ticket is at first glance similar to the negotiability status flag recited in Claim 36. However, the claimed function of the negotiability status flag is not the same as an In Use field of a ticket and, in particular, there is no teaching or suggestion in Rosen of setting a negotiability status flag for buyer and seller document carriers to "negotiable" and "non-negotiable" following a successful END transfer.

The sessions established in Rosen are symmetric cryptographic sessions (see above) whether it is money or a ticket which is being transferred. By contrast, claim 36 recites using the public encryption key of the buyer's document carrier to encrypt a message comprising the END together with the negotiability status flag. This encryption, using a public encryption key, is by definition an asymmetric encryption process fundamentally different to the symmetric cryptographic sessions which Rosen teaches are to be established in transferring either money or a ticket between trusted agents. It is noted that when transferring a ticket, a digital signature is appended by the sender (column 7, lines 56-59; column 26, line 28), but this is in addition to the preceding information on the ticket and for verification of the sender – the encrypting is performed by the symmetric key cryptographic links illustrated in Figure 13 and described with reference to the Establish Session sub routine outlined above.

It is therefore submitted that the method of negotiating an END recited in independent Claim 36 is neither taught nor suggested by Rosen, and it is further noted that

none of the additionally cited prior art documents provide any motivation for the skilled person to adopt a technique different to that taught by Rosen. In particular, the Examiner will recognize that the Establish Session protocols taught by Rosen to establish the secure cryptographic sessions illustrated in Figure 13 are fundamental to the procedure employed by Rosen (for example, because each entity provides half the symmetric key) and thus any modification of this part of the procedure would effectively eviscerate the technical content of the Rosen specification.

Independent Claim 37

Similar points can be made in relation to Claim 37 as are made in relation to Claim 36 above. Broadly speaking, Claim 37 recites a "counter indicative of a number of times that an END has been negotiated since issue" instead of the negotiability status flag, performing a different check (that the counter has a different value) and following a successful transfer incrementing the counter by one).

As the Examiner acknowledges, Rosen does not disclose such a counter. Furthermore, it is submitted that the skilled artisan would have no incentive to consider such a counter and the possibility of duplication etc. is addressed by the abort and commit protocol mentioned above.

In the rejection of Claim 37, the Examiner cites Pitroda (US 5,590,038), column 2, lines 55-61, column 15, lines 58-63 and column 16, lines 39-40, but it is respectfully submitted that all this discloses is that a unique serial number for a card may be provided. There is no teaching or suggestion of a "counter indicative of a number

of times that an END has been negotiated since issue". The Examiner also refers to Abraham (US 5,148,481), in particular column 5, lines 5-55, column 2, lines 1-5 and column 1, lines 60-65. However none of these references, it is respectfully submitted, either teaches or suggests a counter indicative of a number of times that an END has been negotiated since issue – the only reference to a counter appears to be in column 5, but here it is simply employed as a random number generator (column 5, lines 5-7), a counter apparently being employed so that the same random number is not provided twice. It is further noted that "it is not important that the counter actually counts [upward] in the conventional sense" (column 5, lines 13-14).

It is therefore respectfully submitted that even if all three prior art documents, Rosen, Pitroda, and Abraham are combined there is nothing in such a combination to either teach or suggest the subject matter of Claim 37. It is further noted that at point (2) made in respect of Claim 36 above also applies and provides a further very significant, and it is respectfully submitted patentable, distinction over the prior art.

Dependent Claims Dependent Upon Claims 36 and 37

Claims 38 to 45 and 52 to 59 are patentable by virtue of their dependence upon independent Claim 36 or 37, for the reasons given above.

The Examiner's provisional view regarding the patentability of the features particularly recited in these dependent claims is also respectfully contested.

Independent Claim 60

The Examiner acknowledges that Rosen does not explicitly show electronically splitting an END into two or more parts and then negotiating those parts separately to one or more further buyers. The Examiner refers to Halter (US 5,319,705), in particular column 4, lines 23-52 and Figure 2 with an initial opinion that this document discloses such electronic splitting and separate negotiation. However, a careful reading of the cited passage shows that this document, in fact, makes no mention of either splitting an END electronically into two or more parts or negotiating those parts separately to one or more further buyers. Instead, Halter describes a method of tracing customer keys to customers by assigning a unique customer number to each customer, but it entirely silent on splitting an electronic negotiated document, let alone making any mention of what to do with such a document once split. It is therefore respectfully submitted that the combination of Rosen and Halter neither teaches nor suggests the subject matter of this claim.

Dependent Claim Dependent upon Claim 60

The Examiner's provisional view regarding the patentability of dependent Claim 61 is further respectfully contested and it is also submitted that this dependent claim is patentable by virtue of its dependence upon Claim 60.

Accordingly and for the foregoing reasons, claims 25 to 61 should be allowed and we request reconsideration to that end.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

John F. McKenna
Reg. No. 20,912
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500